OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

# Cyber Threat Framework (Version 4)

## Translating Cyber into English

LEADING INTELLIGENCE INTEGRATION

# We both speak English?

- Apartment
- French Fries
- Elevator
- Gasoline
- Soccer
- Cookie

- Flat
- Chips
- Lift
- Petrol
- Football
- Biscuit

# What You Need to Know

- Define Cyber Threat Framework
- Recognize the benefits of using standardized language to describe cyber activity and enable consistent categorization
- Understand the Cyber Threat Framework hierarchy and its four layers of information
- Understand how the Cyber Threat Framework can be used to support analysis

# Cyber Threat Framework (CTF) Overview

The Cyber Threat Framework was developed by the US Government to enable consistent characterization and categorization of cyber threat events, and to identify trends or changes in the activities of cyber adversaries. The framework captures the adversary life cycle from (a) “PREPARATION” of capabilities and targeting to (b) initial “ENGAGEMENT” with the targets or temporary nonintrusive disruptions by the adversary to (c) establishing and expanding the “PRESENCE” on target networks, to (d) the creation of “EFFECTS and CONSEQUENCES” from theft, manipulation, or disruption. The framework categorizes the activity in increasing “layers” of detail (1- 4) as available in the intelligence reporting.

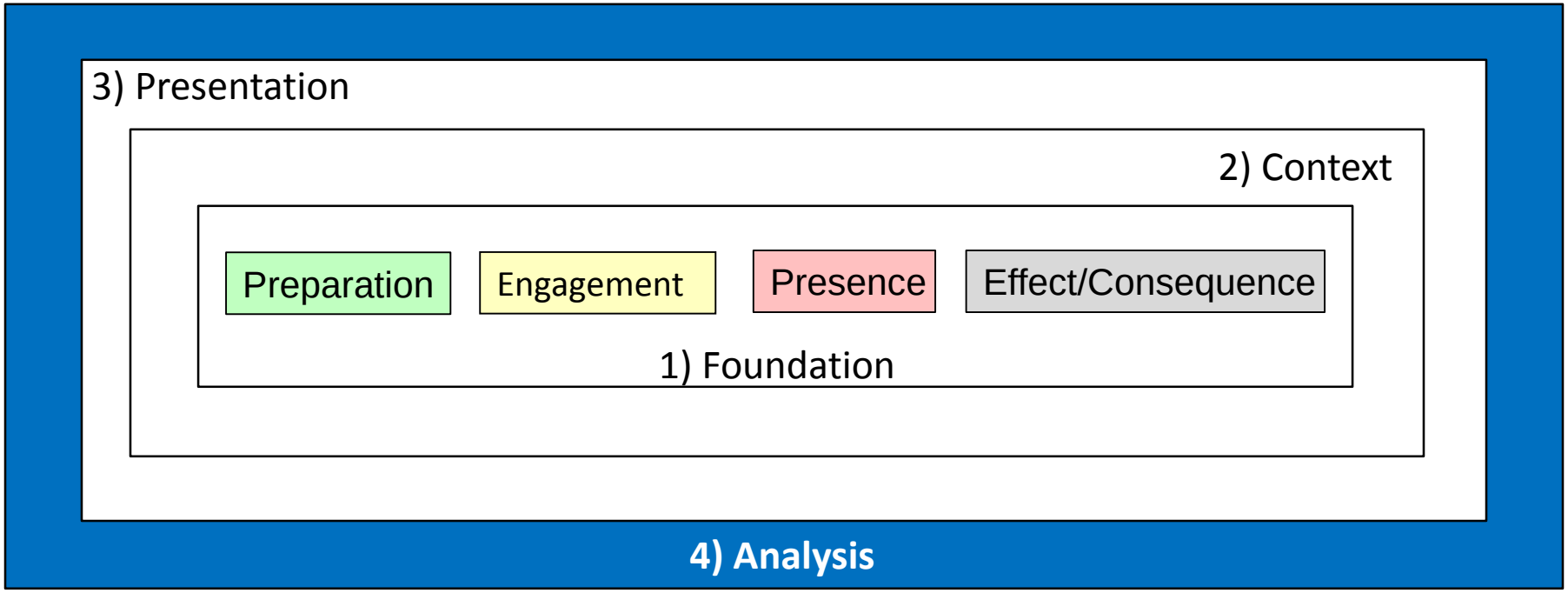
# There are many cyber threat models or frameworks – *why build another*?

- Began as a construct to enhance data-sharing throughout the US Government
- Facilitates efficient situational analysis based on objective (typically, sensor-derived) data
- Provides a simple, yet flexible, collaborative way of characterizing and categorizing activity that supports analysis, senior-level decision making, and cybersecurity
- Offers a common backbone ('cyber Esperanto'); easier to map unique models to a common standard than to each other
- Facilitates cyber threat trend and gap analysis, and assessment of collection posture

# Merging Disparate Data Layers into a Common Framework is a Standard Practice

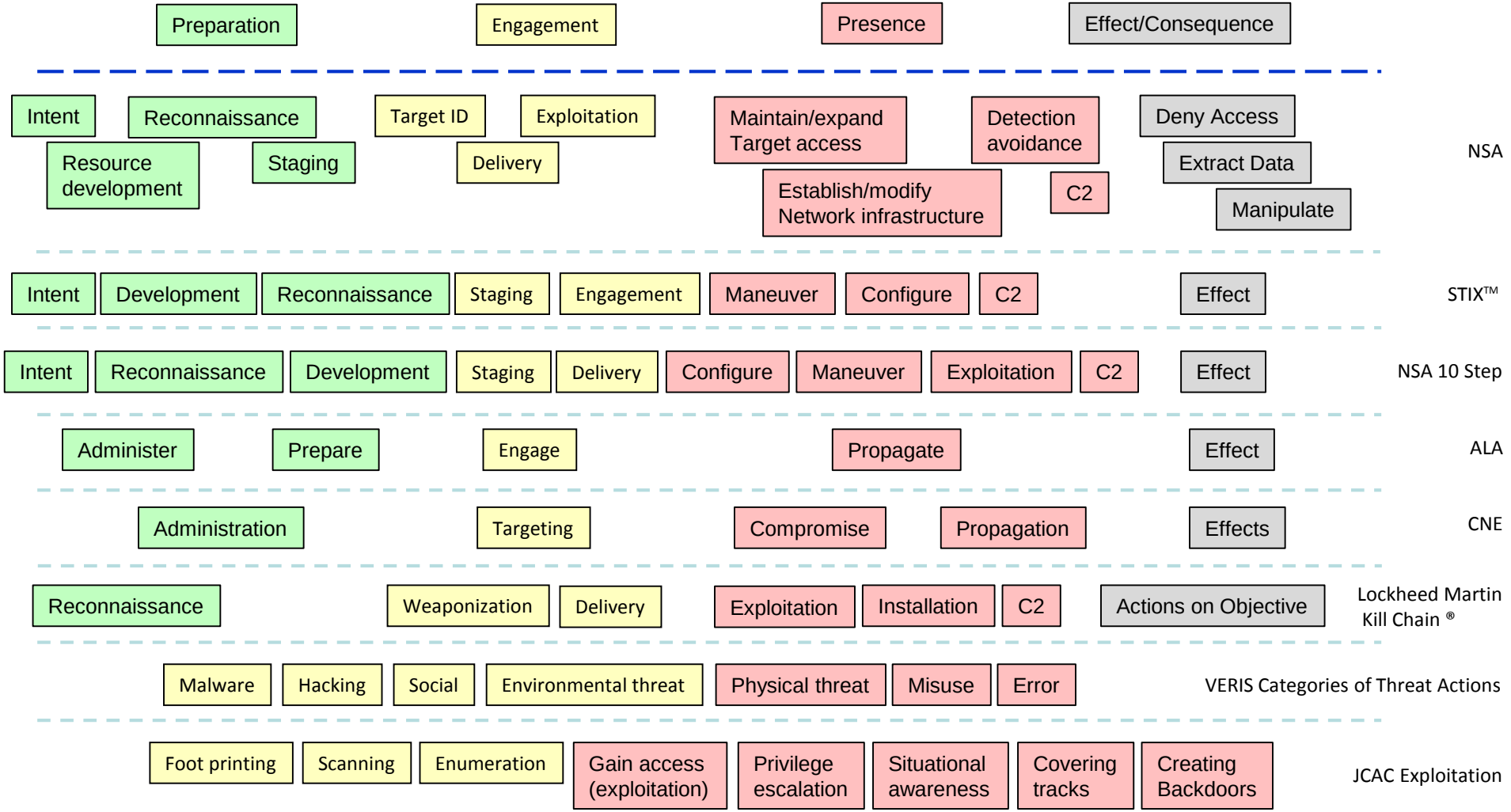
- Weather – overlaying satellite (clouds), doppler (rain), and thermometer (temperature) data atop a map yields a forecast: "take your umbrella and wear a light coat"
- Air Traffic Control – integrating weather, regional/ground control radars, scheduling data, aircraft/ground handler status to control air traffic: "you are cleared to land"
- In a similar fashion, a cyber threat framework based on measurable data facilitates visualization, analysis, and realization of a Common Operating Picture of threat activity
- It can also be matched with other data layers (e.g., vulnerability, shared connections) to become more actionable

# Cyber Threat Framework Evolution

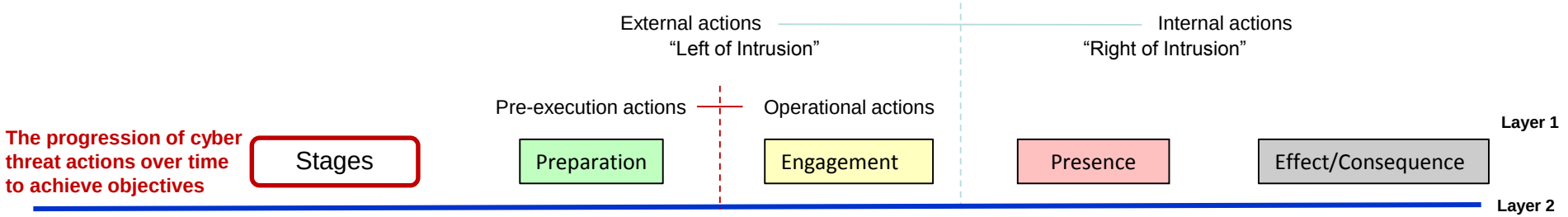



1) Created consensus around a foundation
2) Added context to validate linkages and demonstrate that you could move up and down the framework
3) Developed presentation models
4) Current focus – encompass analytics and automation

# Deriving a 'Best of Breed' Common Framework



# Cyber Threat Framework Layer 1




- Threat activity based on measurable/observable actions
- Every victim and all reported activity accounted for
- Layered data hierarchy providing activity traceability

# CTF Layer 1 Definition – Preparation

Preparation

- Activities undertaken by a threat actor, their leadership and/or sponsor to prepare for conducting malicious cyber activities, e.g., establish governance and articulating intent, objectives, and strategy; identify potential victims and attack vectors; securing resources and develop capabilities; assess intended victim's cyber environment; and define measures for evaluating the success or failure of threat activities.

# CTF Layer 1 Definition – Engagement

Engagement

- Threat actor activities taken prior to gaining but with the intent to gain unauthorized access to the intended victim's physical or virtual computer or information system(s), network(s), and/or data stores.

# CTF Layer 1 Definition – Presence

Presence

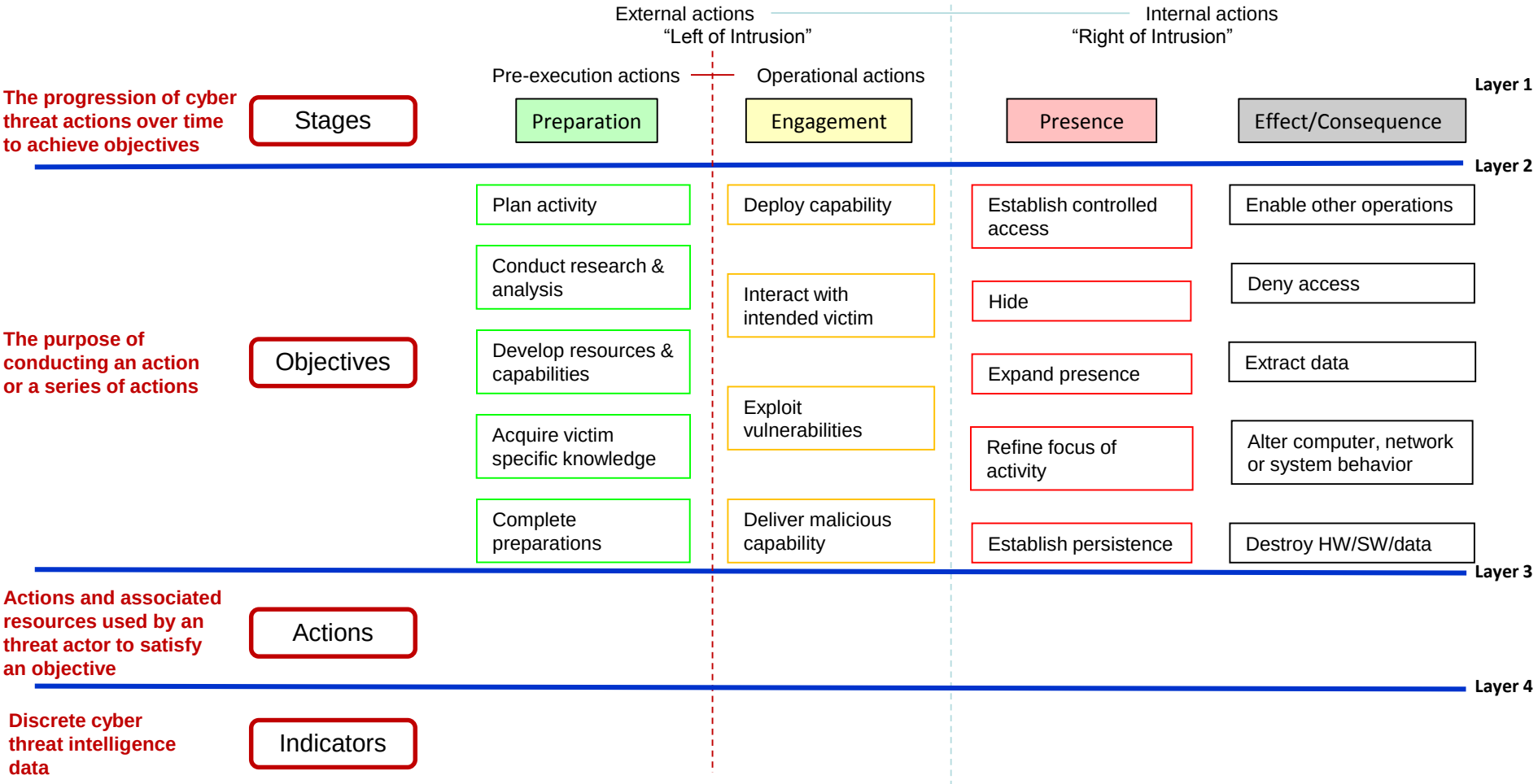
- Actions taken by the threat actor once unauthorized access to victim(s)' physical or virtual computer or information system has been achieved that establishes and maintains conditions or allows the threat actor to perform intended actions or operate at will against the host physical or virtual computer or information system, network and/or data stores.

# CTF Layer 1 Definition – Effect/Consequence

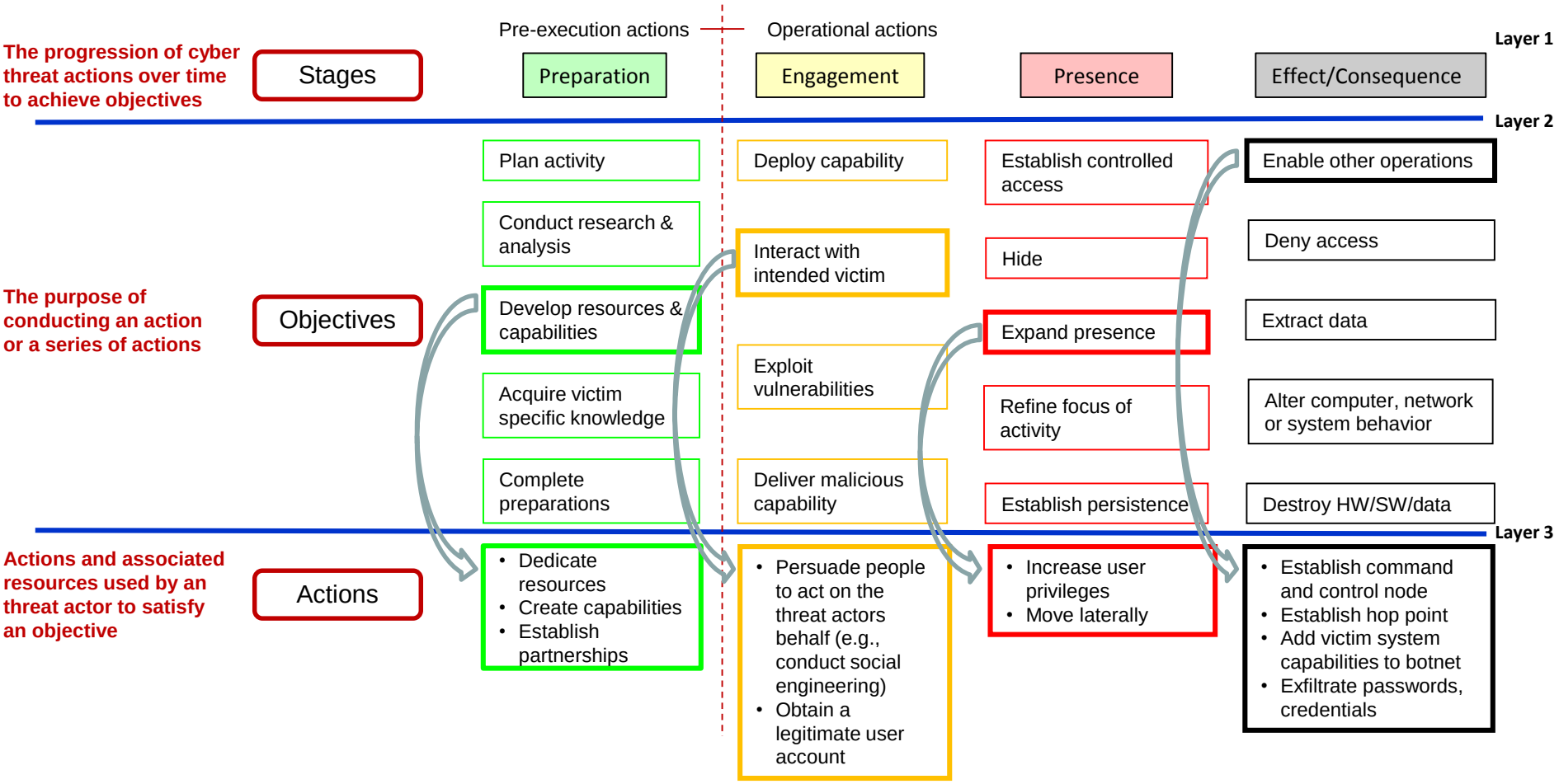
Effect/Consequence

- Outcomes of threat actor actions on a victim's physical or virtual computer or information system(s), network(s), and/or data stores.

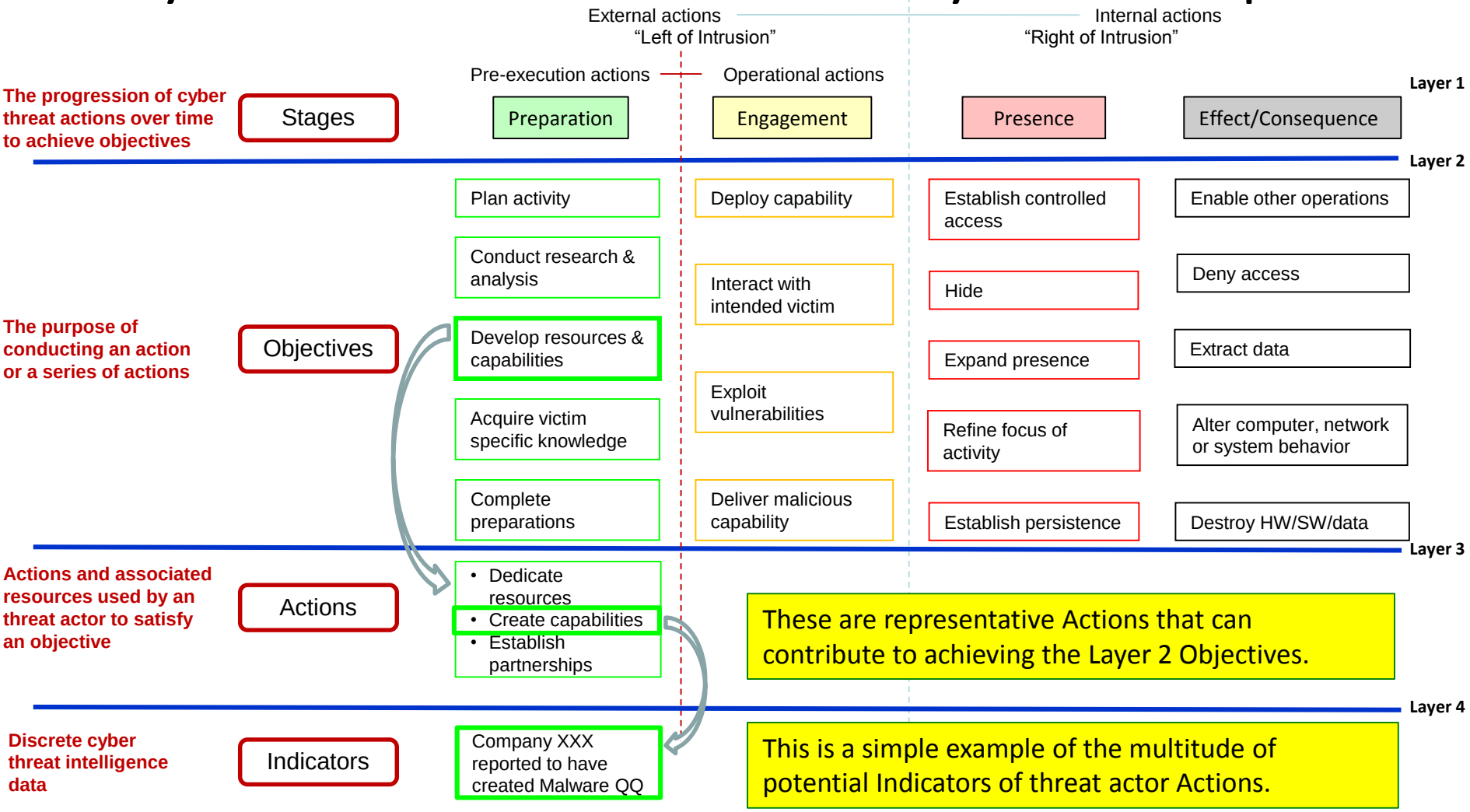
# Cyber Threat Framework (v4) Layer 2 Details



# Cyber Threat Framework (v4) Layer 3 Exemplars



# Cyber Threat Framework (v4) Layer 4 Exemplar



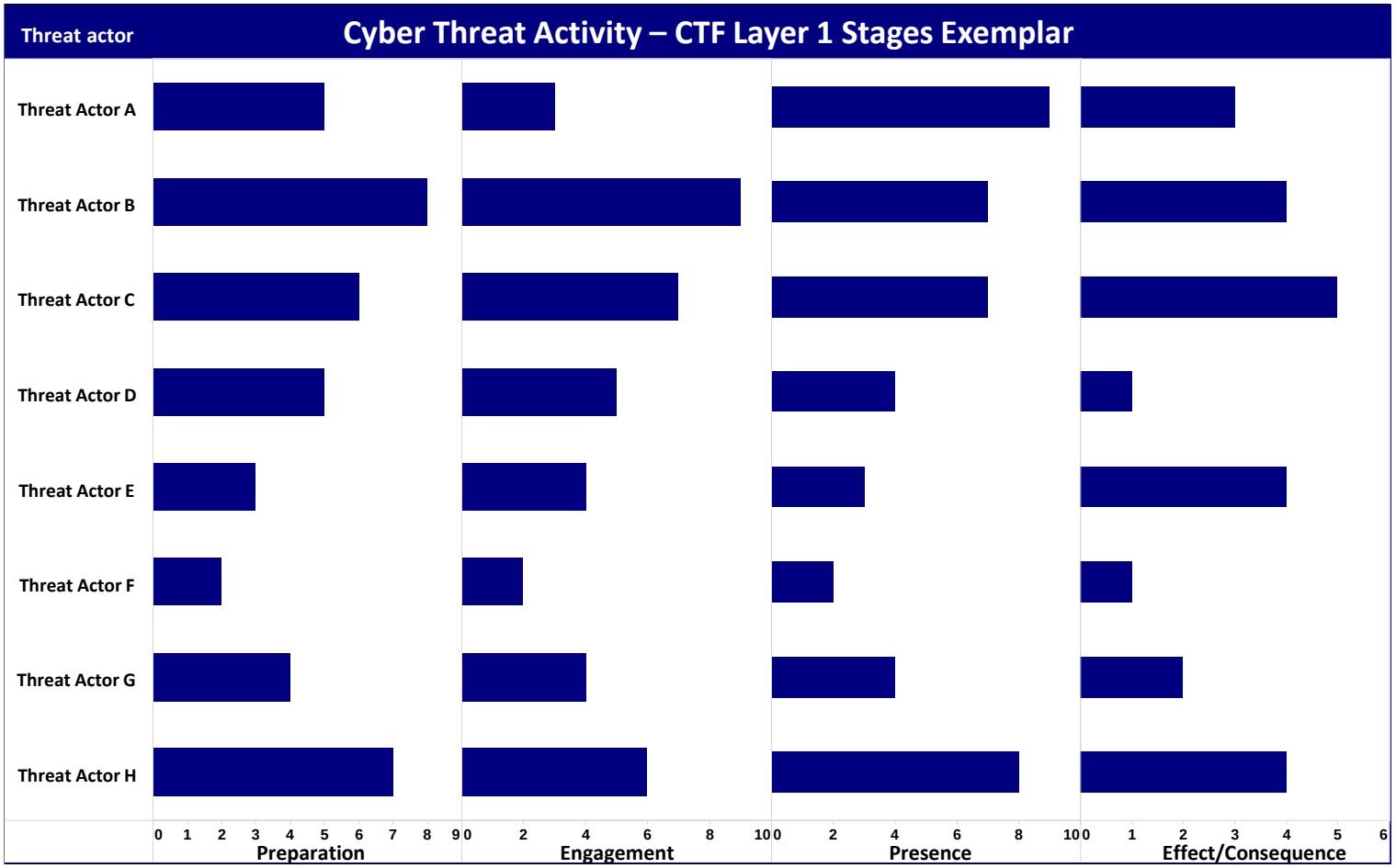
# Consumer Needs Dictate Perspective and Content

- The foundation, based on empirical data, is the common reference point for all subsequent views
  - The consumer provides the focus by defining the view and/or adjusting the type of content (actor, activity, targeted sector, and victim)
  - The consumer defines the required granularity in each view but can "drill down" to see the underlying detail as desired
- The framework is applicable to a range of threat actors, activity, targeted sectors, and victims

# Analysis

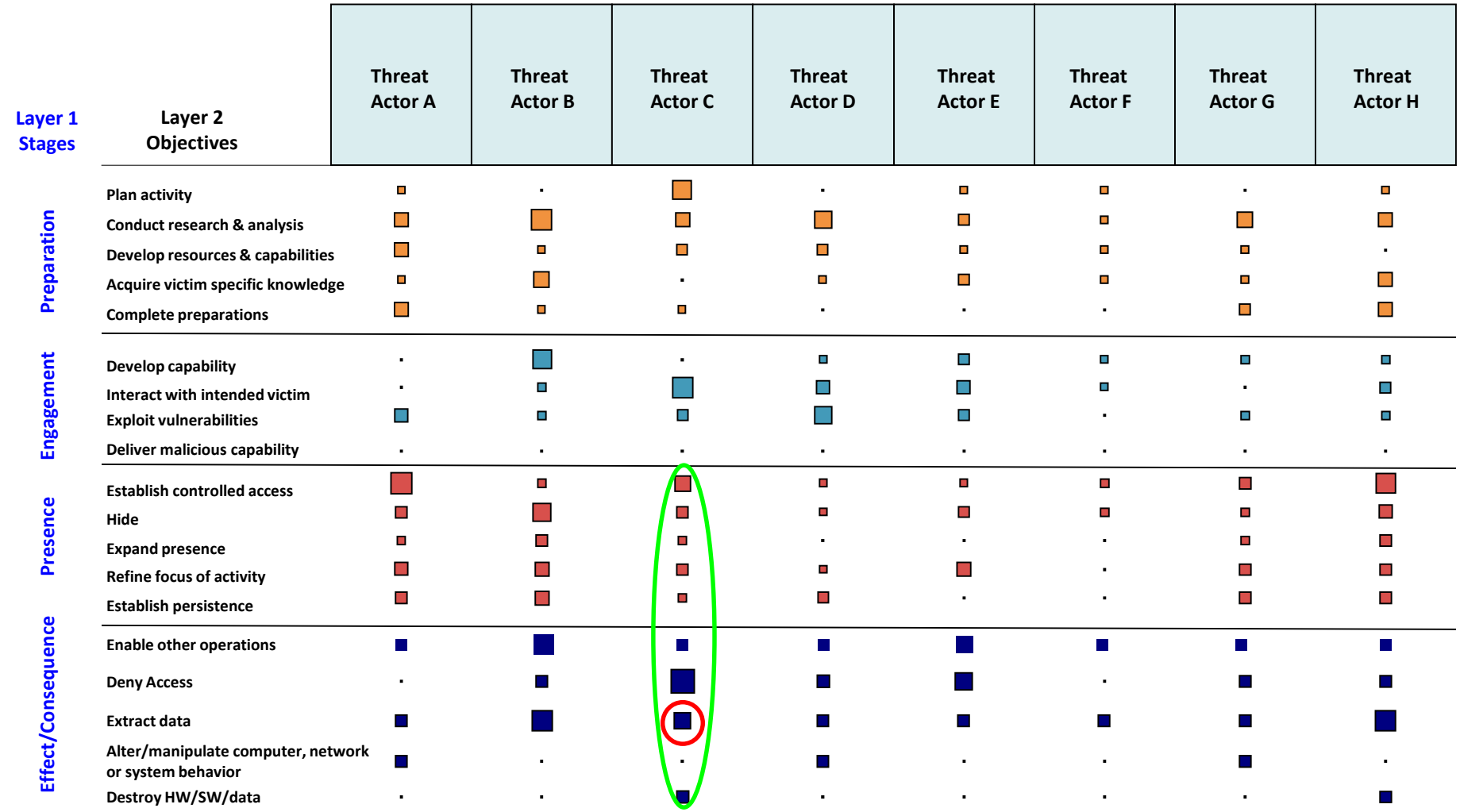
- Depending on the information selected and its presentation, one can begin to conduct a variety of analysis:
  - Trends – change over time
    - What caused the change
  - Predictive – what's next
  - Environmental
    - Was the threat different than expected
    - What vulnerabilities were missed
    - How to optimize remedial action
  - Vulnerability – risk analysis
  - Defensive posture

Threat Actor | Preparation | Engagement | Presence | Effect/Consequence




**Reporting Period: January – March 2016**

# CTF (v4) Layer 2 Objectives Exemplar



# Summary

- The Cyber Threat Framework supports the characterization and categorization of cyber threat information through the use of standardized language.
- The Cyber Threat Framework categorizes the activity in increasing “layers” of detail (1- 4) as available in the intelligence reporting.
- The Cyber Threat Framework can be used to support analysis

Questions?